

Characterization of fiducial states in prime dimensions via mutually unbiased bases

D. Goyeneche,* R. Salazar, and A. Delgado

*Departamento de Física, Universidad de Concepción, Casilla 160-C, Concepción, Chile
Center for Optics and Photonics, Universidad de Concepción, Casilla 4016, Concepción, Chile*

In this work we present some new properties of fiducial states in prime dimensions. We parameterize fiducial operators on eigenvectors bases of displacement operators, which allows us to find a manifold Ω of hermitian operators satisfying $\text{Tr}(\rho) = \text{Tr}(\rho^2) = 1$ for any ρ in Ω . This manifold contains the complete set of fiducial pure states in every prime dimension. Indeed, any quantum state $\rho \geq 0$ belonging to Ω is a fiducial pure state. Also, we present an upper bound for every probability associated to mutually unbiased decomposition of fiducial states. This bound allows us to prove that every fiducial state tends to be mutually unbiased to the maximal set of mutually unbiased bases in higher prime dimensions. Finally, we show that any ρ in Ω minimizes an entropic uncertainty principle related to the second order Rényi entropy.

Keywords: SIC-POVM, Mutually unbiased bases, Weyl-Heisenberg group

I. INTRODUCTION

A symmetric informationally complete positive-operator-valued measure (SIC-POVM) is a set of d^2 rank-one projectors acting on a d -dimensional Hilbert space such that the Schmidt product among any two projectors equals $1/(d+1)$ [1]. The statistic of measurement outcomes associated to a SIC-POVM allows to characterize unambiguously any pure or mixed quantum state. The continued interest on this subject originates in the many important practical applications of SIC-POVMs to quantum mechanics [2], quantum information [3] and to classical signal processing, as well as its possible relation to a better understanding of the structure of the quantum state space [4]. Currently, there exist analytical constructions in $d = 2, 3$ [5], 4, 5 [6], 6 [7], 7 [8], 8 [9], 9, ..., 13, 15 [10], 16 [11] and 19 [8], and high precision numerical solutions in all dimensions $d \leq 67$ [12].

SIC-POVMs have been characterized as d^2 equiangular lines through the origin in \mathcal{C}^d , tight complex projective 2-designs, maximally equiangular tight frames [12], and as simplexes in the Bloch space [13]. Here, our study is restricted to Weyl-Heisenberg covariant SIC-POVMs. These are constructed by applying the generators of the Weyl-Heisenberg group onto a special *fiducial* pure quantum state. We decompose this fiducial state as a combination of projectors onto eigenvectors of the displacement operators. In the particular case of prime dimensions, these eigenvectors form $d+1$ mutually unbiased (MU) bases. Using Zauner's conjecture we obtain a manifold Ω determined by the complete set of *fiducial operators* parameterized by variables such that any fiducial pure state leading to a Weyl-Heisenberg covariant SIC-POVM is contained within this set. We show that any ρ in Ω satisfies $\text{Tr}(\rho) = 1$ and $\text{Tr}(\rho^2) = 1$ and that these operators have the same geometric properties of fiducial states. Fiducial pure states can be singled out by reaching the global maximum of the function $\text{Tr}(\rho^3)$, with ρ in Ω . Thereby, SIC-POVMs are naturally described as a variational problem within the set Ω . We also show that every hermitian operator ρ in Ω minimizes an entropic uncertainty principle and, in particular, the fiducial states. Finally, we deduce an upper bound for each probability defining a fiducial state in the MU bases decomposition. As consequence of this upper bound, fiducial pure states tend to be mutually unbiased to the maximal set of mutually unbiased bases existing in prime dimensions.

II. SIC-POVMS AND DISPLACEMENT OPERATORS

If it is possible to reconstruct every quantum state from a tomographic measurement over a set of operators forming a POVM we say that it is an informationally complete POVM (IC-POVM). The most interesting case of IC-POVM is given by the SIC-POVM, because the overlap of information and errors propagation are minimized. A SIC-POVM is a positive-operator-valued measure formed by d^2 linearly independent rank-one projectors M_k

*Electronic address: dardo.goyeneche@cefop.udec.cl

with $k = 0, \dots, d^2 - 1$, acting on \mathcal{C}^d , that satisfy the property

$$\text{Tr}(M_k M_r) = \frac{d\delta_{k,r} + 1}{d + 1}, \quad (1)$$

for every $k, r = 0, \dots, d^2 - 1$. Considering the projecting directions we can study the equivalent problem to find d^2 pure quantum states $|\phi_k\rangle$ instead of d^2 projectors. That is, assuming that $M_k = |\phi_k\rangle\langle\phi_k|$ then the inner product between two arbitrary states must fulfill the property

$$|\langle\phi_k|\phi_r\rangle|^2 = \frac{d\delta_{k,r} + 1}{d + 1} \quad \forall k, r = 0, \dots, d^2 - 1. \quad (2)$$

There is a strong conjecture that simplifies the way to construct SIC-POVMs. In order to introduce this conjecture let us define first the displacement operators in finite dimension, given by

$$D_{\mathbf{p}} = \tau^{p_1 p_2} X^{p_1} Z^{p_2}, \quad (3)$$

where $\mathbf{p} = (p_1, p_2) \in \mathbb{Z}_d^2$ and $\tau = -e^{i\pi/d}$. The operators X and Z are the *shift* and *phase* operators, defined by

$$X|k\rangle = |k + 1\rangle, \quad Z|k\rangle = \omega^k |k\rangle, \quad (4)$$

where $\omega = e^{2\pi i/d}$, $k = 0, \dots, d - 1$ and $\{|k\rangle\}$ is the canonical (computational) base. If $d = 2$, the displacement operators are the Pauli matrices plus the identity. These operators form, up to a multiplicative constant factor, the generalized Pauli group or Weyl-Heisenberg group. Their commutation rule is given by

$$D_{\mathbf{p}} D_{\mathbf{q}} = \tau^{\langle\mathbf{p}, \mathbf{q}\rangle - \langle\mathbf{q}, \mathbf{p}\rangle} D_{\mathbf{q}} D_{\mathbf{p}}, \quad (5)$$

where $\langle\mathbf{p}, \mathbf{q}\rangle = p_2 q_1 - q_2 p_1$ is a symplectic form. As we can see in the above equation, two displacement operators commute if and only if $\langle\mathbf{p}, \mathbf{q}\rangle = \langle\mathbf{q}, \mathbf{p}\rangle$. Let us now assume that d is a prime number. It is easy to show that

$$D_{\mathbf{p}} = \begin{cases} \tau^{p_2 - p_1 p_2} (D_{\tilde{\mathbf{p}}})^{p_1} & \text{when } p_1 \neq 0, \\ (D_{(0,1)})^{p_2} & \text{when } p_1 = 0, \end{cases} \quad (6)$$

where $\tilde{\mathbf{p}} = (1, p_2 p_1^{d-2})$ and all operations are modulo d . Notice that the d^2 displacement operators can be written as a function of $d + 1$ of them. Of course, the functions must be non linear, because all the operators are linearly independent. The eigenvector basis of the displacement operators in prime dimensions are a maximal set of $d + 1$ MU bases. [14].

Zauner's conjecture [6] states that in every dimension d there exists a *fiducial* state $|\phi\rangle$ such that $\{D_{\mathbf{p}}|\phi\rangle\}$ determines a SIC-POVM. That is,

$$|\langle\phi|D_{\mathbf{p}}|\phi\rangle|^2 = \frac{d\delta_{\mathbf{p},\tilde{0}} + 1}{d + 1} \quad \forall \mathbf{p} \in \mathbb{Z}_d^2. \quad (7)$$

If a pure quantum state $|\phi\rangle$ satisfies the previous condition, then the SIC-POVM is given by $\{D_{\mathbf{p}}|\phi\rangle, \mathbf{p} \in \mathbb{Z}_d^2\}$. If such a construction is possible we say that the SIC-POVM is covariant under Weyl-Heisenberg group.

III. FIDUCIAL STATES IN MU BASES DECOMPOSITION

Any quantum state ρ acting on a prime dimensional Hilbert space \mathcal{H} can be written as a linear combination of rank-one projectors related to a complete set of $d + 1$ mutually unbiased bases. That is,

$$\rho = \sum_{j=0}^d \sum_{k=0}^{d-1} \left(p_k^j - \frac{1}{d + 1} \right) \Pi_k^j, \quad (8)$$

where

$$p_k^j = \text{Tr}(\rho \Pi_k^j), \quad (9)$$

with j the index of the MU bases family and k the index within the family. We consider that $j = d$ corresponds to the canonical base (eigenvectors of Z). Sometimes, this base is denoted with the index $j = \infty$ (see [15]) and this choice is justified by arguments about the discrete affine plane picture [16]. Every operator Π_k^j is a rank one projector, namely

$$\Pi_k^j = |\varphi_k^j\rangle\langle\varphi_k^j|, \quad (10)$$

where $\{|\varphi_k^j\rangle\}$ satisfy the relationship

$$|\langle\varphi_k^j|\varphi_r^l\rangle|^2 = \begin{cases} \frac{1}{d} & \text{when } j \neq l, \\ \delta_{k,r} & \text{when } j = l, \end{cases} \quad (11)$$

that is, they form a complete set of $d + 1$ MU bases. It is also possible to decompose a quantum state as a linear combination of the displacement operators

$$\rho = \sum_{\mathbf{p} \in \mathbb{Z}_d^2} a_{\mathbf{p}} D_{\mathbf{p}}, \quad (12)$$

where $a_{\mathbf{p}} \in \mathbb{C}$ and $a_{\mathbf{0}} = 1/d$. Zauner's conjecture given in Equation (7) can be cast now in the form

$$|\text{Tr}(\rho D_{\mathbf{p}})|^2 = \frac{d\delta_{\mathbf{p},\tilde{\mathbf{0}}} + 1}{d + 1} \quad \forall \mathbf{p} \in \mathbb{Z}_d^2. \quad (13)$$

Considering Equations (12) and (13) and the fact that set $\{D_{\mathbf{p}}\}$ of displacement operators form an orthogonal base we obtain

$$a_{\mathbf{p}} = \begin{cases} \frac{1}{d} & \text{when } \mathbf{p} = \mathbf{0}, \\ \frac{1}{d\sqrt{d+1}} \omega^{\beta_{\mathbf{p}}} & \text{when } \mathbf{p} \neq \mathbf{0}. \end{cases} \quad (14)$$

for a given set of real parameters $\beta_{\mathbf{p}} \in [0, d)$. It is easy to show that the following completeness relation holds

$$\sum_{\mathbf{p} \in \mathbb{Z}_d^2} \frac{1}{d} D_{\mathbf{p}} \rho D_{\mathbf{p}}^{\dagger} = \mathbb{I}, \quad (15)$$

for any set $\{\beta_{\mathbf{p}}\}$. In order to deduce a relationship between the set of coefficients $\{p_k^j\}$ given by Equation (8) and the set of coefficients $\{a_{\mathbf{p}}\}$ given by Equation (12) we need an expression of the displacement operators as a function of the MU bases projectors. Taking into account that every operator $D_{\mathbf{p}}$ has the same set of eigenvalues $\{\omega^k\}$ (with $k = 0, \dots, d-1$) we obtain

$$D_{\mathbf{p}} = \begin{cases} \tau^{p_2 - p_1 p_2} \sum_{k=0}^{d-1} \omega^{kp_1} \Pi_k^{\tilde{p}_2} & \text{when } p_1 \neq 0, \\ \sum_{k=0}^{d-1} \omega^{kp_2} \Pi_k^0 & \text{when } p_1 = 0. \end{cases} \quad (16)$$

Putting Equations (16) into Equation (12) and considering Equation (14) we have

$$\begin{aligned} \rho &= \sum_{p_2=1}^d \sum_{k=0}^{d-1} \frac{1}{d(d+1)} \Pi_k^{p_2} \\ &+ \sum_{p_2=1}^d \sum_{k=0}^{d-1} \sum_{p_1=1}^{d-1} a_{(p_1, p_1 p_2)} \tau^{p_1 p_2 - p_1^2 p_2} \omega^{kp_1} \Pi_k^{p_2} \\ &+ \sum_{k=0}^{d-1} \left(\frac{1}{d(d+1)} + \sum_{p_2=1}^{d-1} a_{p_2} \omega^{kp_2} \right) \Pi_k^0. \end{aligned} \quad (17)$$

From the last result and considering Equation (14), we have the following relationship

$$p_k^j = \frac{1}{d} + \frac{1}{d\sqrt{d+1}} \sum_{r=1}^{d-1} \omega^{\alpha_r^j + kr}, \quad (18)$$

for every $j = 0, \dots, d$ and $k = 0, \dots, d-1$, where the $d^2 - 1$ phases have the form

$$\omega^{\alpha_r^j} = \begin{cases} \omega^{\beta_{(r, jr)}} \tau^{jr - jr^2} & \text{when } j \neq 0, \\ \omega^{\beta_{(0, r)}} & \text{when } j = 0, \end{cases} \quad (19)$$

Given that every probability p_k^j is a real number and considering that d is an odd prime number we find the symmetry

$$\alpha_r^j = -\alpha_{d-r}^j. \quad (20)$$

for every $j = 0, \dots, d$ and $r = 1, \dots, d-1$. Therefore, Equation (18) is reduced to

$$p_k^j = \frac{1}{d} + \frac{2}{d} \sqrt{\frac{1}{d+1}} \sum_{r=1}^{(d-1)/2} \cos(\alpha_r^j + 2\pi kr/d). \quad (21)$$

This characterization of the probability distributions for fiducial operators in MU bases decomposition is our first result. Let us note that the normalization conditions are implicit in the last equation. Additional non-trivial restrictions to the phases $\{\alpha_r^j\}$ can be obtained from considering $0 \leq p_k^j$ on Equation (21), that is

$$-\frac{\sqrt{d+1}}{2} \leq \sum_{r=1}^{(d-1)/2} \cos(\alpha_r^j + kr), \quad (22)$$

whereas $p_k^j \leq 1$ gives us a trivial upper bound. All operators ρ given by Equation (8) with probability distributions $\{p_k^j\}$ given by Equation (21) build the manifold Ω . Any operator in Ω can be used to construct a set of d^2 operators satisfying Equations (13) and (15). However, we cannot guarantee the existence of quantum states in Ω , that is, positive semidefinite operators of unitary trace. Indeed, a fiducial state ρ expressed in Equation (8) must be pure. An adequate set of phases $\{\alpha_r^j\}$ such that $\rho \geq 0$ and $\rho \in \Omega$ give us a fiducial pure state. Another way to show this is by considering the following proposition [17]:

PROPOSITION III.1 *Let $|\phi\rangle$ a quantum state belonging to a d -dimensional Hilbert space with d prime and let $\{p_k^j\}$ the set of $d+1$ probabilities distributions associated to $|\phi\rangle$. Then, $|\phi\rangle$ is fiducial if and only if the following conditions hold*

1. $\sum_{k=0}^{d-1} (p_k^j)^2 = \frac{2}{d+1}, \forall j = 0, \dots, d.$
2. $\sum_{k=0}^{d-1} p_k^j p_{k+r}^j = \frac{1}{d+1}, \forall r = 1, \dots, d-1.$

It is easy to show that any $\rho \in \Omega$ satisfies the conditions (i) and (ii) for every prime dimension. However, we cannot prove that Ω contain pure states. This is the reason why we do not prove the existence of fiducial states in prime dimensions.

IV. PURITY CONDITIONS

Any operator contained in the set Ω is hermitian but not necessarily a quantum state. Our interest here is to find a reduced number of conditions over the phases $\{\alpha_r^j\}$ to single out in Ω a pure quantum state. The following proposition helps to this end [18]:

PROPOSITION IV.1 *Let ρ be an hermitian operator, and suppose that $\text{Tr}(\rho^2) = \text{Tr}(\rho^3) = 1$. Then, ρ is a rank-one projector.*

Let us note that if $\text{Tr}(\rho) = 1$ and $\text{Tr}(\rho^2) = 1$ the only way to have a positive semidefinite operator ρ is that $\text{Tr}(\rho^3) = 1$. If this does not hold, then ρ has one negative eigenvalue, at least. This fact is easy to understand because the only quantum states having $\text{Tr}(\rho^2) = 1$ are the pure states. In our case, $\text{Tr}(\rho) = 1$ is implicit in the MUBs decomposition given in Equation (8). We can also easily deduce from Equation (18) that

$$\sum_{j,k} (p_k^j)^2 = 2, \quad (23)$$

for every value of the phases $\{e^{i\alpha_r^j}\}$. On the other hand, it is known a general property relating probabilities in MUBs decomposition with the purity of a quantum state [19], namely:

$$\sum_{j,k} (p_k^j)^2 = \text{Tr}(\rho^2) + 1. \quad (24)$$

Combining the last two equations we obtain

$$\text{Tr}(\rho^2) = 1. \quad (25)$$

Thus, condition 1) of Proposition IV.1 is implicit in the probability distributions $\{p_k^j\}$ given by Equation (21). Therefore, we only need to impose the condition

$$\text{Tr}(\rho^3) = 1, \quad (26)$$

in order to have a pure state in Ω . Taking into account Equation (26) and the MU bases decomposition given in Equation (17) we obtain

$$\sum_{\substack{j \ l \ r \\ k \ m \ s}} p_k^j p_m^l p_s^r \text{Tr}(\Pi_k^j \Pi_m^l \Pi_s^r) = \text{Tr}(\rho^3) + d + 6, \quad (27)$$

which must be satisfied by the probability distributions $\{p_k^j\}$ (depending on $\{\alpha_k^j\}$) to guarantee that they represent a physically admissible fiducial pure state. Equation (27) indicates that the problem of the existence of Weyl-Heisenberg covariant SIC-POVMs is equivalent to demonstrate that the function

$$F(\{p_k^j\}) = \sum_{\substack{j \ l \ r \\ k \ m \ s}} p_k^j p_m^l p_s^r \text{Tr}(\Pi_k^j \Pi_m^l \Pi_s^r) \quad (28)$$

achieves a maximum value of $d + 7$ for some ρ in Ω . We can affirm that the maximum value belongs to the interval $[d + 5, d + 7]$, but so far we have not been able to proof that $F = d + 7$ is reached for every prime dimension d . Numerical evidence tells us that this maximal number is reached in Ω in every dimension $d \leq 67$ [12] and, consequently, we have a strong evidence of its existence in every prime dimension.

Let us establish an upper bound for the probabilities p_k^j . From Equation (21) we can bound the cosines, obtaining

$$p_k^j \leq \frac{1}{d} + \frac{d-1}{d} \sqrt{\frac{1}{d+1}}, \quad (29)$$

for every $k = 0, \dots, d-1$ and $j = 0, \dots, d$. This bound is highly non-trivial and it may be useful to reduce computational time in order to find numerical solutions in higher dimensions. Another interesting property is that any $\rho \in \Omega$ minimizes the total quadratic Rényi entropy

$$T = \sum_{j=0}^d H_j = - \sum_{j=0}^d \log_2 \left(\sum_{k=0}^{d-1} (p_k^j)^2 \right). \quad (30)$$

Considering Equation (18) we obtain the minimal quadratic Rényi entropy as a function of the dimension d only, that is

$$T = (d+1) \log_2 \left(\frac{d+1}{2} \right). \quad (31)$$

This result is a consequence of the convexity of the logarithm, Jensen's inequality and Equation (18). The total quadratic Rényi entropy is useful to define an entropic uncertainty principle, as we can see in [17]. In the same work, it was shown that fiducial states in prime dimensions are minimum uncertainty states if the total uncertainty $T = \sum_{j=0}^{d-1} H_j$ is considered. Here, we have found that any hermitian operator $\rho \in \Omega$ minimizes this uncertainty principle.

V. SUMMARY

We have studied the problem of constructing Weyl-Heisenberg covariant SIC-POVMs in prime dimensions. Considering useful properties of the displacement operators we have constructed a $(d^2 - 1)/2$ -dimensional manifold Ω of hermitian operators ρ that contains the complete set of Weyl-Heisenberg covariant fiducial operators. Any $\rho \in \Omega$ satisfy $\text{Tr}(\rho) = 1$ and $\text{Tr}(\rho^2) = 1$. The existence of fiducial pure states $\rho \in \Omega$ is equivalent to show that the global maximum $\text{Tr}(\rho^3) = 1$ is attainable in every dimension for some $\rho \in \Omega$. Finally, we also deduced an upper bound for each probability of a fiducial operator in MU bases decomposition in prime dimension and proved that any operator $\rho \in \Omega$ minimizes an entropic uncertainty principle. This allow us to think fiducial states as *coherent states* in prime dimensions [17]. We would like to conclude by noting a connection between fiducial states and entanglement: The matrix operators in Ω can be map onto a set $\tilde{\Omega}$ in a d^2 -dimensional product space L by concatenating one row after the other. This lineal space L can be decomposed as $L_1 \otimes L_2$, where both L_1 and L_2 are d -dimensional and elements in the canonical base of L are identified with tensor products of elements in the canonical bases of L_1 and L_2 . It turns out that an operator in Ω is a fiducial pure state if and only if it corresponds to a separable vector of $\tilde{\Omega}$ in $L_1 \otimes L_2$. We hope our results, together with very well known properties of the pure/separable states manifold, help us to proof the existence of SIC-POVMs in every prime dimension without finding explicit expressions for them.

VI. ACKNOWLEDGMENTS

This work was supported by Grants CONICyT PFB-0824, MSI P10-030-F, and FONDECyT Grants N° 1080383 and N° 3120066. R. S. acknowledges support from CONICyT.

-
- [1] Renes J, Blume-Kohout R, Scott A and Caves A 2010 *J. Math. Phys.* **45** 2171.
 - [2] Scott A 2006 *J. Phys. A* **39** 13507.
 - [3] Medendorp A, Torres-Ruiz F, Shalm L, Tabia G, Fuchs C and Steinberg A 2011 *Phys. Rev. A* **83** 051801.
 - [4] Appleby D, Flammia S and Fuchs C 2011 *J. Math. Phys.* **52** 022202.
 - [5] Delsarte P, Goethals J and Seidel J Philips 1975 *Res. Rep.* **30** 91.
 - [6] Zauner G 1999 *Quantendesigns – Grundzüge einer nichtkommutativen Designtheorie*, Ph. D. thesis, Universität Wien.
 - [7] Grassl M 2004 *Preprint* quant-ph/0406175.
 - [8] Appleby D 2005 *J. Math. Phys.* **46** 052107.
 - [9] Grassl M 2005 *Tomography of quantum states in small dimensions*, Proc. Workshop on Discrete Tomography and its Applications (City University of New York, June, 2005) *Electron. Notes Discrete Math.* **20** 151.
 - [10] Grassl M 2008 *Computing equiangular lines in complex space*, in Mathematical Methods in Computer Science: Essays in Memory of Thomas Beth (Universität Karlsruhe, December, 2008), *Lecture Notes in Computer Science* **89** 5393 .
 - [11] Appleby D, Bengtsson I, Brierley S, Grassl M, Gross D and Larsson J 2011 *Quant. Inf. and Comp.*, vol. 12, 0404.
 - [12] Scott A and Grassl M 2010 *J. Math. Phys.* **51** 042203.
 - [13] Salazar R, Goyeneche D and Delgado A 2011 *Phys. Lett. A*, Volume 376, Issue 4, p. 325-329.
 - [14] Bandyopadhyay S, Boykin P, Roychowdhury V and Vatan F 2002 *Algoritmica* **34** 512; *Preprint* quant-ph/0103.162
 - [15] Appleby D 2009 *Found. of Prob. and Phys.* 5 Book Series: AIP Conf. Proc. **1101** 223-232 *Preprint* quant-ph/0905.1428v1
 - [16] Gibbons K, Hoffman M and Wootters W 2004 *Phys. Rev. A* **70** 062101.
 - [17] Appleby D, Dang H and Fuchs C 2010 *Preprint* quant-ph/0707.2071v2
 - [18] Jones N and Linden N 2005 *Phys. Rev. A* **71** 012324.
 - [19] Larsen U 1990 *J. Phys. A: Math. Gen.* **23** 1041.